InfoCage モバイル防御
管理者ガイド

InfoCage モバイル防御
Version 3.62
管理者ガイド

はじめに

このたびは、NEC の InfoCage モバイル防御をお買い求めいただき誠にありがとうございます。InfoCage モバイル防御は、パソコンからの情報漏洩を防止するセキュリティソフトウェアです。
ご使用になる前に本書をよくお読みになり、製品の取り扱いを十分にご理解ください。

● 商標について

- Microsoft および Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- InfoCage は日本電気株式会社の登録商標です。
- その他、本マニュアルに記載されている会社名、商品名は各社の商標または登録商標です。
- このマニュアルの一部、又は全部を流用・複写することはできません。
- 本マニュアル中のサンプル画面で使用している名称は、全て架空のものです。実在する品名、団体名、個人名とは一切関係ありません。

● 免責事項

本書及び本システムは、ライセンス契約に基づいて使用することができます。ライセンス契約で明示的に定められていないかぎり、日本電気株式会社は製品、及びその関連文書について、明示的にも暗黙的にも、商品性に関する保証、特定目的への適合性に関する保証、取り扱い、使用、または取引行為に伴う保証について一切の責任を負いません。

本書について

本書は、InfoCage モバイル防御の導入前に行うセットアッププログラムのカスタマイズ手順を記載しています。
InfoCage モバイル防御をカスタマイズする際にご利用ください。
カスタマイズが完了した後は、『InfoCage モバイル防御 インストールガイド』を参照してインストールしてください。

本文中の記号について

本文中では、説明、操作手順の他に以下の記号を利用しています。これらの記号の意味を正しくご理解になり、本書をお読みください。

項目	説明
⚠Notice	システムの取り扱いで守らなければならない事柄や特に注意すべき点、確認すべき点を説明します。
参照	関連する内容が記載されているページを紹介しています。

用語の定義

本書では、システム操作の説明に以下のような用語を用いています。
本書を確認するにあたって前提としてご理解ください。

項目	説明
InfoCage モバイル防御	パソコンからの情報漏洩を防止するため、認証を受けていない人がそのパソコンを使うことを防止したり、データを暗号化して読めないようにしたりすることができる情報漏洩対策セキュリティソフトウェアです。
暗号化	第三者の解読・利用を防ぐために、デジタル情報を組み替えることです。組み替えの際に用いられる特定の情報を「鍵」と呼びます。InfoCage モバイル防御はパソコンのドライブまたはフォルダを暗号化します。 メディア鍵認証方式では、鍵または合鍵などがパソコンに装着された状態、またはネットワーク鍵にアクセスできる状態のいずれかでなければ、暗号化されたハードディスクドライブの中を閲覧することはできません。 パスワード認証方式では、ユーザパスワードを認証しない限り、暗号化されたハードディスクドライブの中を閲覧することはできません。 ただし、Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。
復号	暗号化したファイルを元に戻すことです。
セキュリティ認証	パソコンを操作可能な状態にする際に、アクセスする権利があるかどうかを確認することです。セキュリティ認証を行うと、Windows へログオンしてパソコンを操作できるようになります。これによって、パソコンの不正利用やなりすまし利用を防止します。セキュリティ認証が行われないとパソコンはロックされた状態のため、パソコン内の暗号化されたデータは読み取ることができません。
InfoCage モバイル防御ユーティリティ	InfoCage モバイル防御を使ってパソコンの保護設定を行うためのアプリケーションです。InfoCage モバイル防御をパソコンにインストールして使用します。この InfoCage モバイル防御ユーティリティを起動して、パソコンの保護設定やパスワードの変更、鍵の作成(メディア鍵認証方式)の操作を行います。
メディア鍵認証方式／パスワード認証方式	InfoCage モバイル防御の運用方式です。 インストールの際に、外部メディアを鍵としてパソコンの認証を行うメディア鍵認証方式か、またはパスワードにてパソコンの認証を行うパスワード認証方式を選択します。

項　目	説　明
スーパーバイザパスワード／ユーザパスワード	InfoCage モバイル防御ユーティリティ起動時などに必要なパスワードです。メディア鍵認証方式で運用する場合はスーパーバイザパスワードを、パスワード認証方式で運用する場合はユーザパスワードを使用します。
管理者	InfoCage モバイル防御の管理者をさします。InfoCage モバイル防御のセットアッププログラムのカスタマイズを行います。
クライアント	InfoCage モバイル防御のシステム上で管理者が管理を行うパソコンをさします。
利用者	クライアントを利用する人をさします。
保護対象	暗号化によりデータを保護するパソコンの内蔵ドライブをさします。鍵を作成する際に設定します。（メディア鍵認証方式）
メディア暗号ユーティリティ	USB メモリなどのメディアの中に暗号化したファイルを保存し、これらのファイルを InfoCage モバイル防御のインストールされていないパソコンで復号し、使用するためのユーティリティです。
外部メディア自動暗号	許可された外部メディア（許可外部メディア）へ書き出すときに自動的に暗号化を行う機能です。許可外部メディアは、同じグループ名とキーワードが設定されているパソコンでのみデータを読み書き可能で、許可されていないメディアや他のグループのパソコンではデータの読み書きはできません。
外部メディア	OS がリムーバブルメディアと認識するメディア、フロッピーディスクおよび許可外部メディアのことをさします。
許可外部メディア	外部メディア自動暗号機能によりグループ内で使用が許可されたメディア（CD-R/RW、DVD-R/+R/RW/RAM は対象外）をさします。

目 次

第1章　InfoCage　モバイル防御について

InfoCage　モバイル防御は、パソコンからの情報漏洩を防止するため、認証を受けていない人がそのパソコンを使うことを防止したり、データを暗号化して読めないようにしたりすることができる情報漏洩対策セキュリティソフトウェアです。

1.1　InfoCage　モバイル防御の特徴

InfoCage　モバイル防御は、以下の機能で情報を強固に保護します。

各機能の操作方法については、「InfoCage　モバイル防御　ユーザーズガイド」を参照してください。

● **パソコンのロック**

メディア鍵認証方式の場合

鍵となるメディア等をパソコンから抜くことでパソコンをロックし、操作ができないようにします。
また、鍵をパソコンに装着することでセキュリティ認証が行われ、パソコンのロックを解除できます。

パスワード認証方式の場合

InfoCage モバイル防御のユーザパスワードが正しく入力された場合にセキュリティ認証が行われ、Windows にログオン可能になります。

※ Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。

● **ドライブ、フォルダの暗号化**

InfoCage モバイル防御は、ドライブおよびフォルダ単位で一括して内蔵ドライブ内のデータの暗号化を行います。セキュリティ認証が行われないとパソコン内のデータは暗号化されたままのため、読み取ることができません。

メディア鍵認証方式の場合

鍵となるメディアが装着された場合にセキュリティ認証が行われ、暗号化されたファイルへアクセスが可能になります。

パスワード認証方式の場合

パスワードを正しく入力した場合にセキュリティ認証が行われ、暗号化されたファイルへアクセスが可能になります。

※ Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。

● **外部メディア自動暗号** （InfoCage モバイル防御の管理者による設定が必要）

外部メディア内のデータの暗号化を自動的に行います。所属するグループ内でのみ使用が許可される外部メディア（許可外部メディア）を設定し、この許可外部メディアへはデータは自動的に暗号化されて書き込まれ、読み込むときには自動的に復号されます。

● **メディア暗号ユーティリティ**

USB メモリなどのメディアの中に暗号化して保存したファイルを、InfoCage モバイル防御のインストールされていないパソコンで復号する場合には、メディア暗号ユーティリティを使います。

● **データの抜き取り防止** （メディア鍵認証方式のみ）

認証されていないメディアへのコピーを禁止して、情報の抜き取りを防止します。

● **セキュリティチップ（TPM）でのセキュリティ強化** （InfoCage モバイル防御の管理者による設定が必要）

InfoCage モバイル防御をパスワード認証方式で運用し、セキュリティチップ（TPM）搭載のパソコンをお使いの場合、セキュリティチップ（TPM）と連携し、より強固なセキュリティを実現します。
（WindowsXP のみ）

1.2　鍵とは

InfoCage モバイル防御 メディア鍵認証方式で使用する鍵には以下の 3 種類があります。

● **鍵**

鍵とは、パソコンにログオンする際や暗号化されたデータにアクセスする際などに必要な認証情報をメディア等に作成したものです。鍵がなければドアが開かないのと同様に、鍵として設定したメディアがなければ、セキュリティ認証が行われず、パソコンの情報にアクセスできません。
鍵はメディアやネットワークの共有フォルダに作成できます。

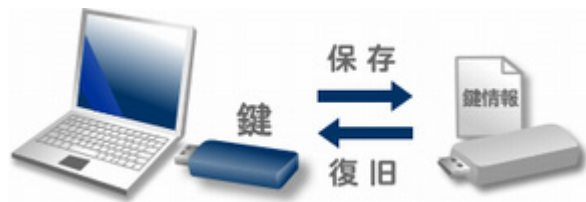
● **合鍵**

合鍵とは、スペアキーのことです。
万が一の鍵の紛失等に備えて、パソコンの保護対象ごとに 1 つの鍵に対して合鍵を 2 つまで作成できます。
鍵または合鍵のうちどれか 1 つで、パソコンやメディアの保護と解除ができます。

● **合成鍵**（WindowsXP／2000 のみ）

異なるメディアに作成した鍵を 2 つ組み合わせて使用するダブルロックキーのことです。
組み合わせることができるのは 2 つまでです。
鍵が 2 つそろわなければパソコンやリムーバブルメディアの保護を解除できません。

1.3　鍵情報とは

鍵のバックアップデータを鍵情報といい、鍵となるメディアとは別のメディアに保存しておきます。
鍵となるメディア内のデータを紛失した場合等は、鍵情報を元に鍵を復旧します。

⚠Notice

鍵情報を紛失すると鍵の復旧ができません。鍵情報を保存したメディア内のデータを絶対に紛失しないように注意してください。

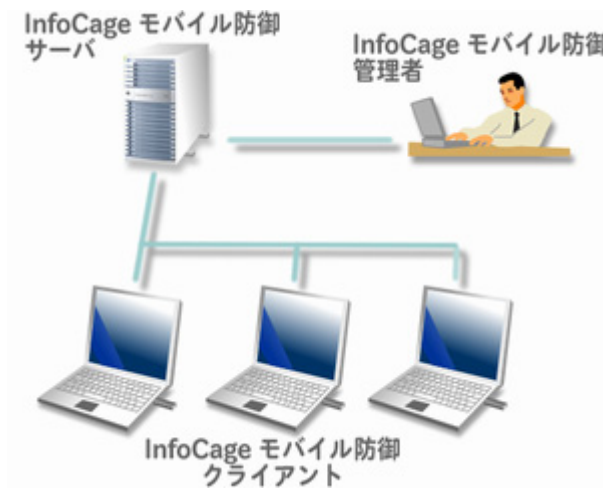
1.4 運用モード

運用モードには、クライアント単体で運用するスタンドアローンモードと、InfoCage モバイル防御の管理者が InfoCage モバイル防御サーバを使ってクライアントの設定などを管理するネットワークモードがあります。
インストール後に運用モードを変更する場合は、運用モード設定ユーティリティを使います。

- **スタンドアローンモード**

クライアント単体で運用します。

- **ネットワークモード**

スタンドアローンモードの機能に加え、InfoCage モバイル防御サーバと連携する運用モードです。
InfoCage モバイル防御の管理者が InfoCage モバイル防御サーバにてユーザ登録やポリシー設定を行い、クライアントの管理などを行います。

1.5　初期暗号化モード

InfoCage　モバイル防御をインストールした後に実行される暗号化は、通常は「ドライブ一括暗号モード」によりドライブ単位で行われます。
ただし、InfoCage　モバイル防御の管理者により「個別暗号モード」に設定されている場合は、指定したドライブおよびフォルダのみ暗号化を行います。

● **ドライブ一括暗号モード（デフォルト）**

● **個別暗号モード**

第2章　セットアッププログラムのカスタマイズ

InfoCage　モバイル防御のセットアッププログラムは、管理者があらかじめ各ツールを使ってカスタマイズすることができます。
カスタマイズすることにより、InfoCage　モバイル防御の管理者が設定したポリシーのもとで運用することができます。
管理者のパソコンで作成したセットアッププログラムや設定ファイルを利用者に配布し、InfoCage　モバイル防御をインストールしてください。

セットアッププログラムをクライアントにインストールする場合は、「InfoCage　モバイル防御　インストールガイド」を参照してください。

2.1　インストールの流れ

InfoCage　モバイル防御は以下の流れでインストールします。

1.　セットアッププログラムのカスタマイズ（InfoCage　モバイル防御の管理者が設定）

カスタマイズ方法は、本ガイドの各章を参照してください。

2.　利用者にセットアッププログラムを配布

セットアッププログラムを配布する際に通知および配布するものは下表を参照してください。

3.　インストール

InfoCage　モバイル防御をインストールします。

インストールについては、「InfoCage　モバイル防御　インストールガイド」を参照してください。

4.　再起動

5.　暗号化ウィザード

・パソコンの鍵および鍵情報を作成します。（メディア鍵認証方式のみ）
・フォルダ／ドライブを暗号化します。

6.　終了

セットアッププログラムを配布する際に、必要に応じて下記を利用者に通知および配布してください。

各 OS に応じたインストールガイド
運用方法の通知（メディア鍵認証方式またはパスワード認証方式）
プロダクト ID の通知
鍵および鍵情報を保存するメディアの配布（メディア鍵認証方式の場合）
暗号化するドライブ／フォルダの通知（個別暗号モードインストールの場合）
許可外部メディアの配布（許可外部メディアを利用する場合）

2.2　サポート対象オペレーティングシステム

オペレーティングシステムによって、InfoCage　モバイル防御の使用できる機能が異なります。
各オペレーティングシステムで使用できる機能は表示アイコンで確認してください。

オペレーティングシステム	表示アイコン
Windows Vista Home Basic （日本語版）	Vista
Windows Vista Business （日本語版）	
Windows Vista Ultimate （日本語版）	
Windows　XP　Professional （日本語版）	XP/2000
Windows　XP　Home Edition （日本語版）	
Windows　XP　Tablet　PC　Edition （日本語版）	
Windows　XP　Tablet　PC　Edition　2005 （日本語版）	
Windows　2000　Professional （日本語版）	

オペレーティングシステムによるInfoCage　モバイル防御の主な機能差は、
「2.5 Windows Vista用とWindows XP/2000 用の機能の違い」を参照してください。

2.3　注意事項

- InfoCage　モバイル防御をインストールするパソコンのオペレーティングシステムによって、使用するツールおよびセットアップの参照場所が異なります。
  ツールやフォルダの参照場所を誤ると、正しく InfoCage　モバイル防御をインストールできませんのでご注意ください。
- InfoCage　モバイル防御をインストールするパソコンによって、オペレーティングシステムや設定内容が異なる場合は、その都度セットアッププログラムを作成してください。
- Windows　XP/2000 のパソコンにインストールした InfoCage　モバイル防御は Windows　Vista 用の InfoCage　モバイル防御へアップグレードインストールができません。またその逆もできません。

2.4　ガイドの参照場所

それぞれのガイドについては、以下を参照してください。

● InfoCage　モバイル防御　インストールガイド
インストールの際に必要な記述があります。必ず参照のうえインストールしてください。
インストールガイドはクライアント　CD-ROM　内の「2K_XP」フォルダまたは「Vista」フォルダ内の「InfoCage　モバイル防御　インストールガイド」を参照してください。

● InfoCage　モバイル防御　ユーザーズガイド
使用の際に必要な記述があります。インストール完了後に必ず参照してください。
スタートメニューの[すべてのプログラム]－[NEC]－[InfoCage　モバイル防御]－[InfoCage　モバイル防御　ユーザーズガイド]　から参照できます。

2.5　Windows Vista 用と Windows XP/2000 用の機能の違い

InfoCage モバイル防御の Windows Vista 用と Windows XP/2000 用では、使用できる機能が異なります。
詳細は下記の表の通りです。

○･･･使用可能　×･･･使用不可　－･･･機能なし

オペレーティングシステム	XP/2000		Vista	
InfoCage モバイル防御の認証方式	メディア鍵	パスワード	メディア鍵	パスワード
運用モード				
スタンドアローンモード	○	○	○	○
ネットワークモード（管理サーバとの通信）	○	○	○	○
メディア鍵認証方式の機能				
パソコンのロック機能の ON／OFF	○	－	○（注 1）	－
抜き取り防止機能	○	－	○	－
指紋認証機能付き USB メディアでのログオン認証	○	－	×	－
パソコンの鍵の作成	○	－	○	－
ネットワーク鍵の作成	○	－	○	－
合鍵の作成	○	－	○	－
合成鍵の作成	○	－	×	－
リムーバブルメディアの鍵の作成	○	－	×	－
フロッピーディスク鍵の作成	○	－	×	－
鍵の復旧（注 2）	○	－	○	－
ネットワーク共有フォルダへの鍵情報保存	○（注 3）	－	×	－
スーパーバイザパスワードの変更	○	－	○	－
パスワード認証方式の機能				
FeliCa 認証	－	○	－	×
TPM との連携	－	○（注 4）	－	×
ユーザパスワードの変更	－	○	－	○
InfoCage モバイル防御 ユーティリティでの暗号化				
ユーティリティでの内蔵ドライブ、フォルダの暗号化	○	○	○	○
ユーティリティでのリムーバブルメディアの暗号化	○	－	×	－
暗号化を推奨するフォルダの暗号化	○	○	×	×
アプリケーションのインストールフォルダの暗号化	○	○	×	×
初期暗号化モードの選択	○	○	○	○
時限消去機能、セーフモードでの起動許可設定				
時限消去機能の設定	○	○	×	×
セーフモードでの起動許可設定	○	○	×（注 5）	×（注 5）
メディアの暗号機能				
メディア暗号ユーティリティ	○	○	○	○
外部メディア自動暗号機能	○	○	○	○
ツール				
バックアップツール	○	○	×（注 6）	×（注 6）
グループ編集ツール	○	○	○	○

（注 1）　Windows Vista ではパソコンのロック機能は常に ON となります。
（注 2）　Windows Vista のパソコンで作成した鍵は Windows XP/2000 のパソコンでは復旧できません。またその逆もできません。
（注 3）　鍵情報をネットワークの共有フォルダに保存する機能は、本ソフトウェア Ver 1 からのアップグレードユーザのみです。
（注 4）　Windows XP のみ使用可能です。
（注 5）　Windows Vista ではセーフモードでの起動は常に許可されます。
（注 6）　Windows Vista では OS 標準のバックアップ機能が使用可能となります。

2.6　モバイル防御 Windows Vista 用と Windows XP/2000 用の互換性

Windows Vista 用の InfoCage モバイル防御と、Windows XP/2000 用の InfoCage モバイル防御では、作成した鍵の復旧や暗号化したメディアがそれぞれで使用できない場合があります。
互換性は下記の表の通りです。

○・・・使用可能　×・・・使用不可

InfoCage モバイル防御のインストール OS	XP/2000	Vista
暗号化設定および鍵を作成した OS	Vista	XP/2000
パソコンの鍵の復旧	×	×
リムーバブルメディアの鍵の復旧	×（注 1）	×
モバイル防御 ユーティリティで暗号化したメディア	×（注 2）	×
メディア暗号ユーティリティで暗号化したメディア	○	○
許可外部メディア	○	○

（注1）Windows Vista ではリムーバブルメディアの鍵は作成できません。
（注 2）Windows Vista ではモバイル防御ユーティリティでリムーバブルメディアは暗号化できません。

2.7　カスタマイズできる内容

1.　セットアッププログラムの詳細設定

クライアント初期設定ツールを使って、InfoCage モバイル防御の初期暗号化モードや暗号化を指定するフォルダなど、セットアッププログラムの詳細な設定を行います。

（設定できる内容）

- 暗号化を指定するフォルダ、暗号化を推奨するフォルダの設定
- 運用モードの設定（スタンドアローンモード／ネットワークモード）
- 初期暗号化モードの選択（ドライブ一括暗号モード／個別暗号モード）
- 鍵および鍵情報の保存先のデフォルトドライブ指定（メディア鍵認証方式の場合）
- セーフモード起動の設定
- 外部メディア自動暗号の設定
- ログオン認証の設定（パスワード認証方式の場合）
- TPM の使用設定（Windows XP／パスワード認証方式の場合）　　　など

初期設定をしない場合は、デフォルト設定でインストールされます。
詳細は、「第 3 章　セットアッププログラムの詳細設定」を参照してください。

2.　FeliCa カードのシステムコード定義ファイルの作成

XP/2000

InfoCage モバイル防御をパスワード認証モードで運用し、Windows のログオンを特定の種類の FeliCa カードで認証する場合、[システムコード定義ファイル作成ツール]を使って、FeliCa カードのシステムコードの作成を行い、クライアントのパソコンに適用させます。

詳細は、「第 4 章 FeliCaカードのシステムコード定義ファイルの作成」を参照してください。

3.　許可外部メディアの作成

XP/2000

クライアント初期設定ツールで外部メディア自動暗号機能を有効にした場合は、許可外部メディア作成ツールで許可外部メディアとするメディアにグループ名とキーワードを設定します。
クライアント設定ツールで設定したグループ名とキーワードが、許可外部メディアに設定されたグループ名とキーワードと一致した場合に、許可外部メディアを使用することができます。
許可外部メディアにデータの書き込みを行うと自動的に暗号化され、読み込むときには自動的に復号されます。

詳細は、「第 5 章 外部メディア自動暗号機能」を参照してください。

第3章　セットアッププログラムの詳細設定

3.1　概要

InfoCage モバイル防御の初期暗号化モードや暗号化を指定するフォルダなど、セットアッププログラムの詳細な設定を行う場合、クライアント初期設定ツールを使って設定します。
管理者のパソコンでポリシーを設定したセットアッププログラムを利用者に配布し、InfoCage モバイル防御クライアントをインストールしてください。

3.2　設定できる内容

設定できる内容は以下の通りです。
オペレーティングシステムによって、使用できる機能が異なりますので、InfoCage モバイル防御をインストールするパソコンのオペレーティングシステムを確認のうえ、設定してください。
複数のオペレーティングシステムがある場合や、パソコンによって設定内容を変更する場合は、その都度セットアッププログラムを作成してください。

設定内容	使用可能 OS	設定しない場合のデフォルト設定（注）
暗号化を指定するフォルダ （デフォルトの暗号化対象）	Vista XP/2000	なし（インストール時に選択）
暗号化を推奨するフォルダ	XP/2000	なし（インストール時に選択）
運用モードの設定 スタンドアローンモード／ネットワークモード	Vista XP/2000	なし（インストール時に選択）
初期暗号化モードの選択 ドライブ一括暗号モード／個別暗号モード	Vista XP/2000	ドライブ一括暗号モード
ドライブ一括暗号モードの設定 全固定ドライブ／システムドライブのみ	Vista XP/2000	全固定ドライブを暗号化する
鍵および鍵情報の保存先のドライブ指定 ※メディア鍵認証方式の場合	Vista XP/2000	なし（インストール時に選択）
セーフモード起動の設定 許可する／禁止する	XP/2000	セーフモードの起動を許可
外部メディア自動暗号の設定 使用する／使用しない	Vista XP/2000	外部メディア自動暗号を使用しない
ログオン認証の設定 パスワード／FeliCa ※パスワード認証方式の場合	XP/2000	パスワードでログオンする
TPM の使用設定 使用する／使用しない ※Windows XP／パスワード認証方式の場合	XP/2000	TPM を使用しない

（注）初期設定をしない場合は、デフォルト設定でインストールされます。

3.3　操作手順

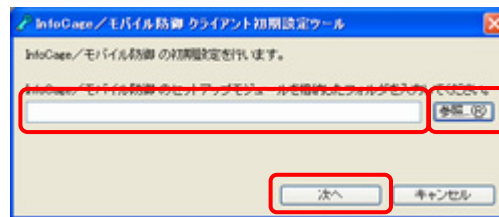
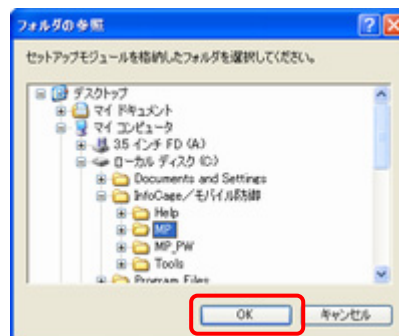
Operation

1. 本ソフトウェアのクライアントCD-ROMの内容をすべて管理者のパソコンの適当なフォルダにコピーしてください。

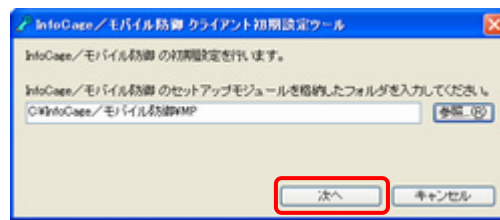
2. 使用する InfoCage モバイル防御の認証方式およびオペレーティングシステムに応じて、CD-ROM 内の以下のファイルを実行してください。

メディア鍵認証方式(Windows XP/2000)	¥2K_XP ¥Tools¥クライアント初期設定ツール¥InitMPCliInst.exe
パスワード認証方式(Windows XP/2000)	¥2K_XP ¥Tools¥クライアント初期設定ツール¥InitMPPWCliInst.exe
メディア鍵認証方式(Windows Vista)	¥Vista ¥Tools¥クライアント初期設定ツール¥InitMPCliInst.exe
パスワード認証方式(Windows Vista)	¥Vista ¥Tools¥クライアント初期設定ツール¥InitMPPWCliInst.exe

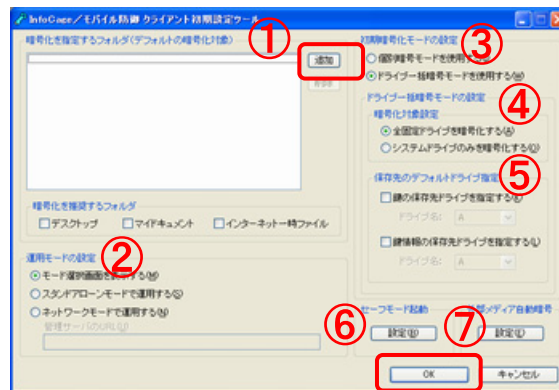
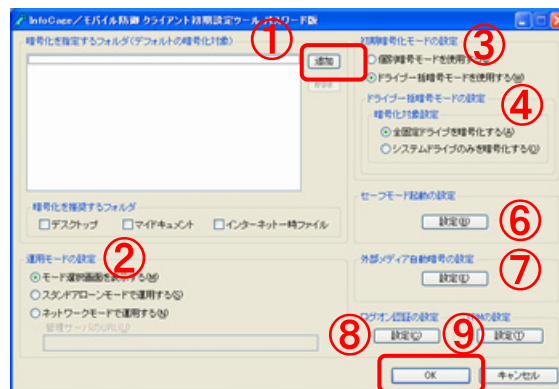
3. 使用する InfoCage モバイル防御の認証方式およびオペレーティングシステムに応じて、*1* でコピーしたフォルダの中から次のパスを入力して「次へ」をクリックしてください。
「参照」をクリックするとフォルダを選択できます。

メディア鍵認証方式(Windows XP/2000)	¥2K_XP¥MP フォルダ
パスワード認証方式(Windows XP/2000)	¥2K_XP¥MP_PW フォルダ
メディア鍵認証方式(Windows Vista)	¥Vista¥MP フォルダ
パスワード認証方式(Windows Vista)	¥Vista ¥MP_PW フォルダ

（参照をクリックした場合）

⚠Notice

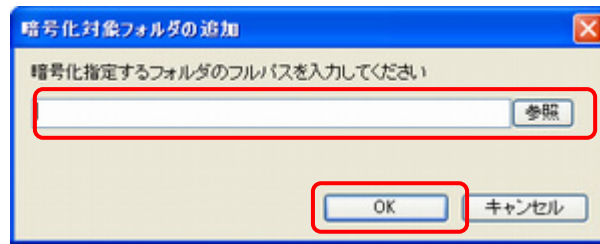
フォルダを間違えると正しく設定できませんのでご注意ください。

4. フォルダのパスを確認して「次へ」をクリックしてください。

5. それぞれ必要な項目を設定し、「OK」をクリックしてください。

> **Notice**
>
> 画面は Windows XP／2000 向けです。Windows Vista 向けは一部異なります。

●メディア鍵認証方式の場合

●パスワード認証方式の場合

①　暗号化を指定するフォルダ（デフォルトの暗号化対象）

すべてのクライアントで暗号化する必要のあるドライブやフォルダをあらかじめ指定することができます。ここで指定したドライブやフォルダは、利用者が設定しなくても、InfoCage モバイル防御をインストール後にユーティリティを起動して暗号化処理を実行することで暗号化されます。

1. システムドライブ以外で暗号化を指定するドライブやフォルダがある場合は、「追加」をクリックしてください。
2. 「参照」をクリックして、暗号化指定するドライブやフォルダを選択するか、管理者のパソコンには存在しないドライブやフォルダを暗号化指定したい場合は、直接パスを入力して設定することもできます。入力できたら、「OK」をクリックしてください。

Notice

- ここで設定したフォルダは③で「個別暗号モードを使用する」を選択した場合に有効になります。
- 暗号化指定するドライブやフォルダが複数ある場合は、1～2 の手順を繰り返してください。
- 以下のフォルダについて暗号化指定する場合は、それぞれのチェックを入れてください。
  (Windows XP／2000 向けのみ)
  ・デスクトップ　　・マイドキュメント　　・インターネット一時ファイル

②　運用モードの設定

クライアントインストール時の運用モード設定画面の表示を設定します。

- モード選択画面を表示する
  クライアントインストール時に、スタンドアローンモードとネットワークモードを選択する場合に選択してください。
  クライアントインストール時に、モードを選択する画面が表示されます。
- スタンドアローンモードで運用する
  全クライアントをスタンドアローンモードで運用する場合に選択してください。
  クライアントインストール時にはスタンドアローンモードでインストールされます。
- ネットワークモードで運用する
  全クライアントをネットワークモードで運用する場合に選択してください。
  クライアントインストール時にはネットワークモードでインストールされます。
  管理サーバの URL を入力しておいた場合、クライアントインストール時に URL が自動で表示されます。

③　初期暗号化モードの設定

インストール方式を設定します。

- 個別暗号モードを使用する
  「個別暗号モード」は、詳細な設定ができるインストール方式です。

Notice

①の「暗号化を指定するフォルダ」を有効にするには、「個別暗号モード」を選択してください。

- ドライブ一括暗号モードを使用する
  「ドライブ一括暗号モード」は、鍵の作成や鍵情報の保存（メディア鍵認証方式のみ）、および暗号化までを InfoCage モバイル防御が推奨する設定で行うインストール方式です。通常はこちらを選択してください。

④　ドライブ一括暗号モードの設定／暗号化対象設定

暗号化対象とするドライブをどちらか選択します。

- 全固定ドライブを暗号化する
  パソコンの内蔵ハードディスクドライブをすべて暗号化するように設定します。
- システムドライブのみを暗号化する
  パソコンの内蔵ハードディスクドライブのうち、システムドライブのみを暗号化するように設定します。

Notice

- ②で「ドライブ一括暗号モード」を選択した場合に有効になります。
- 外部メディア自動暗号機能を使用する場合、暗号化対象としないシステムドライブ以外の内蔵ハードディスクドライブはリムーバブルメディアと同じ扱いとなり、その内蔵ハードディスクドライブへはデータのコピー、移動およびファイルの新規作成ができなくなりますのでご注意ください。

⑤　ドライブ一括暗号モードの設定／鍵の保存先ドライブを指定する

（メディア鍵認証方式の場合のみ）

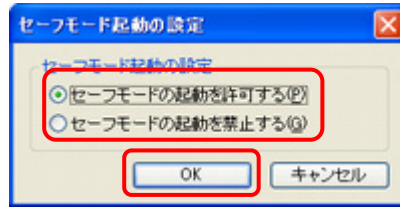
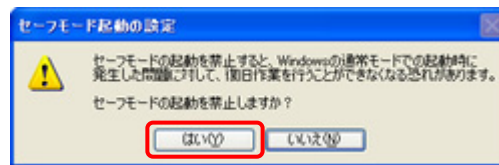
鍵および鍵情報を保存するドライブをあらかじめ指定する場合は、ここで設定します。

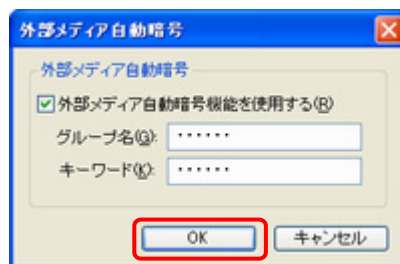
- 鍵の保存先ドライブを指定する
  作成した鍵を保存するドライブを指定する場合、チェックボックスにチェックを入れてドライブを選択してください。
- 鍵情報の保存先ドライブを指定する
  鍵情報を保存するドライブを指定する場合、チェックボックスにチェックを入れてドライブを選択してください。

Notice

②で「ドライブ一括暗号モード」を選択した場合に有効になります。

⑥　セーフモード起動の設定　XP/2000

Windows をセーフモードで起動することを許可するか禁止するかをここで設定します。
「設定」をクリックするとセーフモード起動の設定が表示されますので、どちらかを選択して「OK」をクリックしてください。

「セーフモードの起動を禁止する」を選択した場合、下記のメッセージが表示されます。内容をよく確認して、「はい」をクリックしてください。

⑦　外部メディア自動暗号

外部メディア自動暗号とは、所属するグループ内で許可された外部メディア（許可外部メディア）へデータを書き出すときに自動的に暗号化を行う機能です。グループ名とキーワードを設定することにより、グループ名とキーワードが一致している外部メディアを使用することができます。
外部メディア自動暗号を設定する場合は、「設定」をクリックして「外部メディア自動暗号機能を使用する」にチェックしてください。
また許可外部メディアを所属するグループ内で使用するためのグループ名とキーワードを入力してください。（各全半角 16 文字まで）
入力が完了したら「OK」をクリックしてください。

Notice

- 外部メディア自動暗号機能の概要は、本ガイドの「第 5 章　外部メディア自動暗号機能」の章を参照してください。
- 外部メディア自動暗号機能は、Windows のセーフモードでは有効となりません。大切なデータは必ず暗号化を行ってください。

⑧　ログオン認証の設定（パスワード認証方式の場合のみ）

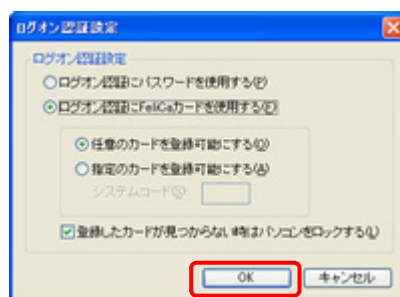
InfoCage モバイル防御をパスワード認証方式で運用する場合、ログオン認証をパスワードまたはFeliCa カードのどちらで認証するかを設定します。

「設定」をクリックしてください。

FeliCa カード認証で認証する場合は、カードの種類を選択します。

- 任意のカードを登録可能にする
  登録するカードの種類を問わない場合に選択してください。

- 指定範囲のカードを登録可能にする
  登録するカードの種類（社員証など）が決まっている場合に選択してください。

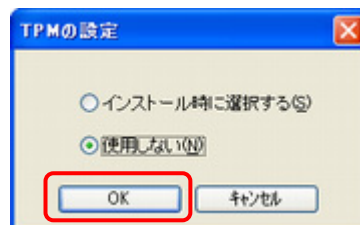
「指定範囲のカードを登録可能にする」を選択した場合はシステムコードを 16 進数 4 文字で入力してください。（0001～fffe まで）
また、FeliCa カードがパソコンにセットされていない場合にパソコンをロックする場合は、「登録したカードが見つからないときはパソコンをロックする」にチェックしてください。
入力が完了したら「OK」をクリックしてください。

⑨　TPM の設定（Windows XP／パスワード認証方式の場合のみ）

InfoCage モバイル防御のパスワード認証方式では、セキュリティチップ（TPM）の機能を使用することにより、さらに強固なセキュリティを実現できます。

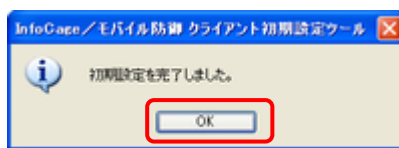
セキュリティチップ（TPM）を使用する場合は、「設定」をクリックしてください。

- インストール時に選択する
  セキュリティチップ（TPM）を使用するかどうかをインストール時にユーザが選択できます。

- TPM を使用しない
  セキュリティチップ（TPM）を使用しません。

どちらかを選択して「OK」をクリックしてください。

Notice

セキュリティチップ（TPM）を使用する場合は、インストールガイドの「セキュリティチップ（TPM）搭載のパソコンをお使いの場合」の章を参照のうえ、使用してください。

6. 確認メッセージが表示されます。「OK」をクリックしてください。

7. ポリシーなどを設定したセットアッププログラムが *1* でコピーした¥MP フォルダまたは¥MP_PW フォルダに作成されていますので、作成したセットアッププログラムを利用者に配布し、インストールガイドにしたがって、各クライアントに InfoCage モバイル防御クライアントをインストールしてください。

Notice

- 初期暗号化モードを個別暗号モードでインストールする場合は、インストールガイドの「個別暗号モード」の章を参照のうえ、セットアップしてください。
- InfoCage モバイル防御をインストールするパソコンのオペレーティングシステムや設定内容を十分確認のうえ、クライアントに配布してください。異なるオペレーティングシステム用のセットアッププログラムを実行することはできません。

第4章 FeliCa カードのシステムコード定義ファイルの作成

4.1 概 要

InfoCage モバイル防御をパスワード認証方式で運用し、ログオン認証に特定の種類の FeliCa カードを使用する場合、[システムコード定義ファイル作成ツール]を使ってシステムコードの定義ファイルを作成し、その定義ファイルをクライアントのパソコンに適用させることで、特定の種類の FeliCa カード認証を有効にします。

Notice

本設定は Windows XP/2000 用の InfoCage モバイル防御をパスワード認証方式で運用する場合に有効な設定です。

4.2 注意事項

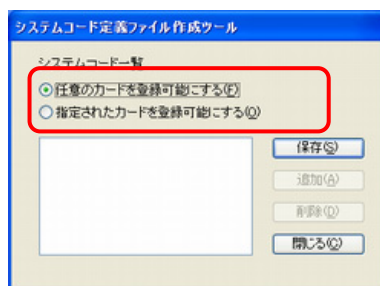
- [システムコード定義ファイル作成ツール]は InfoCage モバイル防御 Ver3.5 以降(Windows XP/2000 向けのみ)がインストールされたパソコンで動作します。
- [システムコード定義ファイル作成ツール]で作成した mbscd.dat ファイルは、[システムコード適用ツール]を使ってクライアントのパソコンに適用してください。
- クライアント初期設定ツールで「ログオン認証に FeliCa カードを使用する」の設定を行ったセットアッププログラムをクライアントのパソコンにインストールする場合は、本設定は必要ありません。

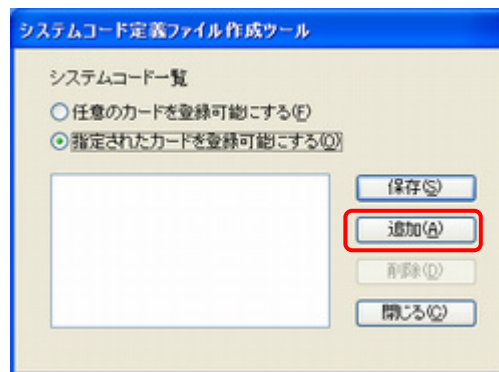
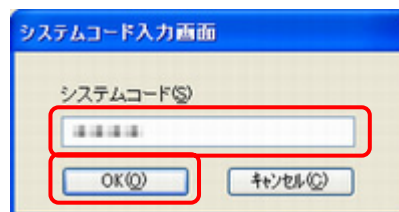
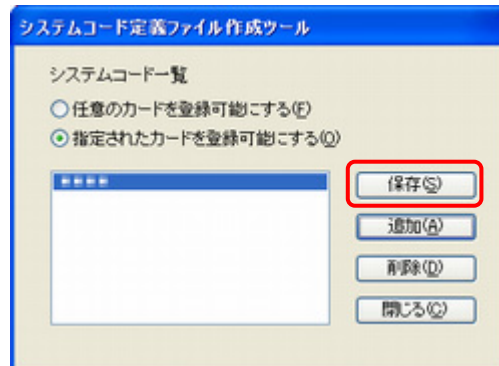
4.3 システムコード定義ファイルの作成

Operation

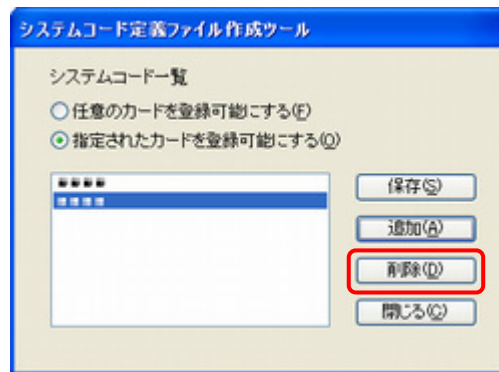
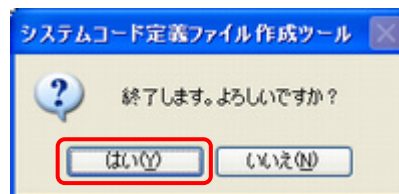
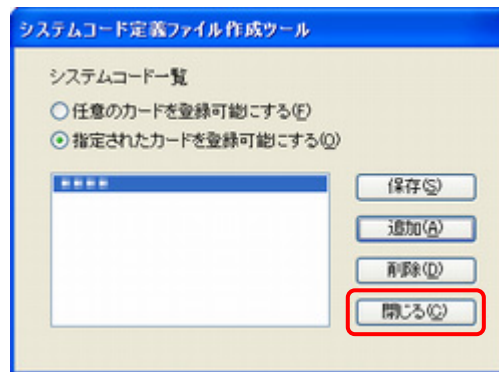
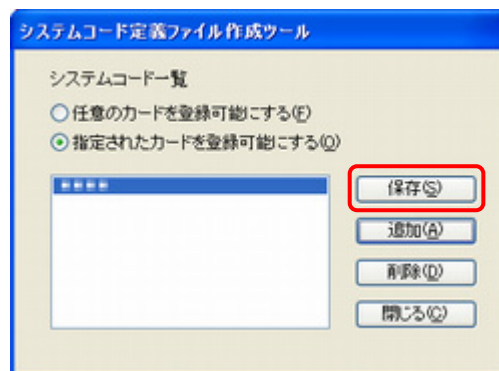
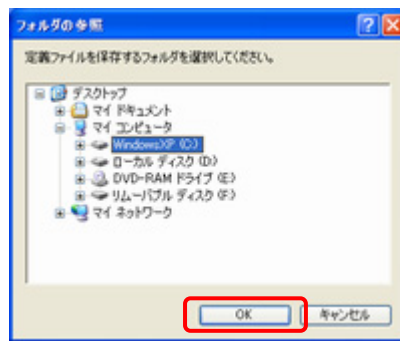
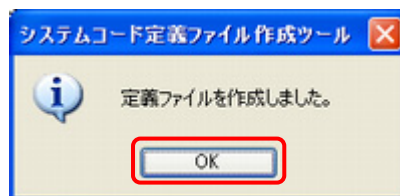
1. クライアント CD-ROM 内の¥2K_XP¥Tools¥システムコード定義ファイル作成ツール フォルダに格納されている NmlMkScd.exe を実行してください。

2. [システムコード定義ファイル作成ツール]が起動します。
「任意のカードを登録可能にする」または「指定範囲のカードを登録可能にする」のどちらかを選択します。

- 任意のカードを登録可能にする
  登録するカードの種類を問わない場合に選択してください。
- 指定範囲のカードを登録可能にする
  登録するカードの種類(社員証など)が決まっている場合に選択してください。

3. 「任意のカードを登録可能にする」を選択する場合は、「保存」をクリックして、*10* へ進んでください。

4. 「指定範囲のカードを登録可能にする」を選択する場合は、「追加」をクリックしてください。

5. 登録するカードのシステムコードを 16 進数 4 文字で入力して、「OK」をクリックしてください。
（0001～fffe まで）

6. システムコード一覧に追加したシステムコードが表示されます。
複数のシステムコードを作成する場合は、*4* ～*5* を繰り返してください。

⚠Notice

システムコードは 8 個まで登録できます。

7. 入力したシステムコードを削除する場合は、削除するシステムコードを選択して「削除」をクリックしてください。一覧から削除されます。

8. 保存せずに終了する場合は、「閉じる」をクリックして終了します。

9. システムコードの入力が完了したら、「保存」をクリックします。

10. 保存する場所を選択して、「OK」をクリックします。

11. 保存を指定した場所に mbscd.dat ファイルが作成されました。「OK」をクリックしてください。
この mbscd.dat ファイルをクライアントに適用します。

以上で操作は完了です。

クライアントのパソコンに登録されているシステムコードを変更する場合は、上記の手順で新しくシステムコード定義ファイルを作成し、クライアントのパソコンに適用させるとシステムコードは変更されます。
クライアントのパソコンにシステムコードを適用する場合は、[システムコード適用ツール]を使って[システムコード定義ファイル作成ツール]で作成したシステムコードをクライアントのパソコンに適用させます。
[システムコード適用ツール]の使用方法は、インストールガイドの「特定の FeliCa カードの設定」の章を参照してください。

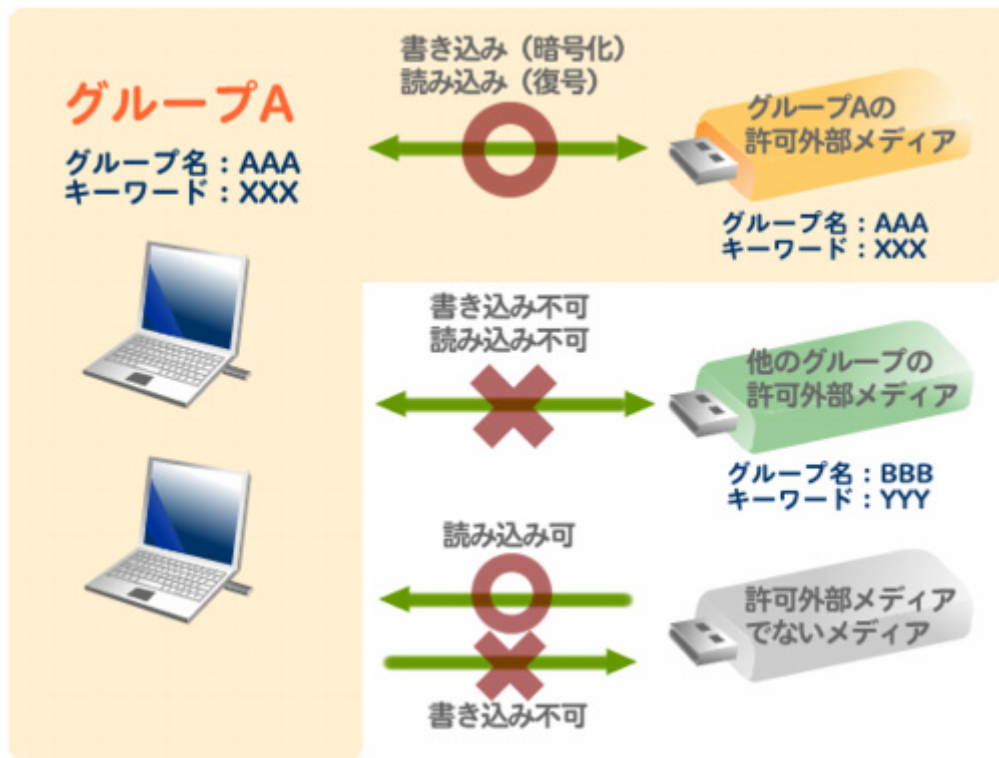
第5章　外部メディア自動暗号機能

5.1　概要

外部メディア自動暗号とは、所属するグループ内で許可された外部メディア（以下「許可外部メディア」という）へデータを書き出すときに自動的に暗号化を行う機能です。
InfoCage モバイル防御の管理者により外部メディア自動暗号が設定された InfoCage モバイル防御をインストールすると、グループおよびキーワードがパソコンに登録され、以下のように許可外部メディアを使用することができます。

(1) 同じグループの許可外部メディア
所属するグループ内で許可されたメディアのみ、データの書き込み／読み込みができます。

(2) 他のグループの許可外部メディア
所属するグループ以外のグループの許可外部メディアは書き込み／読み込みができません。

(3) 許可外部メディアでないメディア
許可外部メディアでないメディアは、データを読み込むことができますが、書き込むことはできません。

5.2　注意事項

- ［許可外部メディア作成ツール］は InfoCage　モバイル防御　Ver3.5 以降がインストールされたパソコンで動作します。
- 本機能を設定した場合は、メディア暗号ユーティリティは使用できません。
  ただし、本機能が設定されている場合でも、タスクトレイに鍵形のアイコンが出ていない状態であれば、メディア暗号ユーティリティを使用できます。
- InfoCage　モバイル防御　ユーティリティが起動しているときは、［許可外部メディア作成ツール］は起動できません。
- リムーバブルメディアの中にデータが存在する場合は許可外部メディアの設定ができません。あらかじめフォーマット等しておいてください。
- リムーバブルメディアとは、OS がリムーバブルタイプと判定するメディアおよびフロッピーディスクを指します。

Notice

CD-R/RW、DVD-R/+R/RW/RAM は対象外となります。

- InfoCage　モバイル防御をメディア鍵認証方式で運用する場合、鍵および鍵情報が格納されたリムーバブルメディアは許可外部メディアにすることはできません。
- Windows XP/2000 のパソコンでメディア鍵認証方式を運用する場合、本設定を行うと InfoCage　モバイル防御　ユーティリティの「全般」タブにある、「認証されていないメディアへのコピーを禁止する」または「メディアへのコピーを禁止する」のチェックは常に ON になります。
- 一度許可設定されたリムーバブルメディアの設定を解除することはできません。許可外部メディアの設定を解除する場合はリムーバブルメディアをフォーマットしてください。
- InfoCage　モバイル防御がインストールされていないパソコンで、許可外部メディアのファイルシステムの変更（FAT および FAT32 から NTFS へのコンバート）を行うと、許可外部メディアの設定が解除されますので、ファイルシステムの変更は行わないでください。
- 本機能をクライアントで使用する場合は、あらかじめ本機能を有効に設定したセットアッププログラムを使ってインストールする必要があります。
  セットアッププログラムの設定は、［クライアント初期設定ツール］で外部メディア自動暗号の設定を行います。

Notice

クライアント初期設定ツールの使用方法は、本ガイドの「第 3 章　セットアッププログラムの詳細設定」の章を参照してください。

- クライアントの所属するグループを変更する場合は、［グループ編集ツール］を使用します。［グループ編集ツール］の使用方法は、ユーザーズガイドの「グループ編集ツールの利用」の項を参照してください。
- グループ内で使用できる許可外部メディアは、グループ名およびキーワードが一致しないと使用できません。（大文字・小文字を区別します）
- 本機能を設定した場合、認証されていない外付けハードディスクドライブ内のファイルを削除する際に表示される「ごみ箱に移しますか？」のメッセージで「はい」をクリックしてもファイルはごみ箱に残らず削除されます。
- Windows XP および Windows 2000 版の InfoCage　モバイル防御で作成した許可外部メディアは、Windows Vista のパソコンで使用が可能です。また Windows Vista 版の InfoCage　モバイル防御で作成した許可外部メディアは、Windows XP および Windows 2000 のパソコンで使用が可能です。
  ただし、オペレーティングシステムによって使用する［許可外部メディア作成ツール］が異なりますので、操作手順にしたがって正しく操作してください。

5.3　操作手順

許可外部メディアの作成方法を説明します。
許可外部メディアとするメディアを準備してください。

Operation

1. グループ名およびキーワードを既定値として許可外部メディア作成ツールに入力する場合は、本ソフトウェアのクライアント CD-ROM 内の以下のフォルダを管理者のパソコンの適当な場所にコピーしてください。

   Windows XP/2000　　¥2K_XP¥Tools¥許可外部メディア作成ツール フォルダ
   Windows Vista　　¥Vista¥Tools¥許可外部メディア作成ツール フォルダ

   > **Notice**
   > 既定値を設定しない場合は、3 に進んでください。

2. 既定値を設定する場合はメモ帳などのテキストエディタで以下のように記述し、nmlmkerm.ini の名前でコピーしたフォルダに保存します。

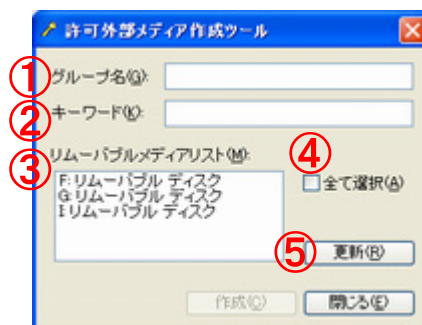
   [default]
   Keyword=<キーワード>　　・・・全半角 16 文字以内
   Groupname=<グループ名>　　・・・全半角 16 文字以内
   Disable =<値>　　・・・グループ名およびキーワードの変更を許可する場合は 0、許可しない場合は 1

   （記述例）
   [default]
   Keyword = InfoCage モバイル防御
   Groupname = グループ 01
   Disable = 1

   > **Notice**
   > Disable =1 の場合は許可外部メディア作成ツール上でキーワードおよびグループ名を変更できません。

3. 許可設定したいリムーバブルメディアを管理者のパソコンに装着します。

4. ¥許可外部メディア作成ツール フォルダ内の NmlMkERM.exe を実行してください。
   [許可外部メディア作成ツール]が起動します。

5. ①～⑤の項目を設定します。

① **グループ名**

[クライアント初期設定ツール]でセットアップに設定したグループ名を入力します。

(全半角 16 文字まで)

> **⚠Notice**
>
> *1* および *2* でグループ名およびキーワードを既定値として設定した場合は既にグループ名およびキーワードが入力されています。

② **キーワード**

[クライアント初期設定ツール]でセットアップに設定したキーワードを入力します。

(全半角 16 文字まで)。

> **⚠Notice**
>
> *1* および *2* でグループ名およびキーワードを既定値として設定した場合は、既にグループ名およびキーワードが入力されています。

③ **リムーバブルメディアリスト**

許可外部メディアとして設定可能なリムーバブルメディアが表示されます。許可するリムーバブルメディアをクリックして選択します。

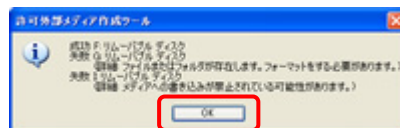
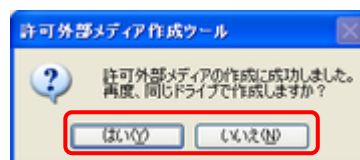
> **⚠Notice**
>
> - 複数のリムーバブルメディアを選択するときは、Ctrl キーまたは Shift キーを押しながらクリックしてください。
> - 鍵および鍵情報が格納されているメディアは許可外部メディアの対象外となりますので、リムーバブルメディアリストには表示されません。

④ **すべて選択**

リムーバブルメディアリストに表示されているメディアをすべて選択する場合は「全て選択」にチェックをつけます。チェックを外すとすべての選択が解除されます。

⑤ **更新**

[許可外部メディア作成ツール]を起動した後にリムーバブルメディアをパソコンに装着した場合など、リムーバブルメディアリストに表示されない場合は「更新」をクリックしてください。

6. *5* の設定が完了し、「作成」をクリックすると許可メディアが設定され、確認メッセージが表示されますので、作成に失敗したメディアはメッセージを確認して「OK」をクリックしてください。

下記のメッセージが表示されたときは、同じドライブで別のリムーバブルメディアを設定する場合は「はい」を、設定を終了する場合は「いいえ」をクリックしてください。

7. 許可外部メディアの設定が完了したメディアはリムーバブルメディアリストの選択が解除されます。選択が解除されていないリムーバブルメディアは、6 のメッセージを確認し、書き込み禁止やメディア内にファイルやフォルダが存在していないこと等を確認し、再度「作成」をクリックしてください。

8. 許可外部メディアの設定が終了したら「閉じる」をクリックし、終了してください。

9. 許可外部メディアを配布してください。

Notice

クライアントでの操作方法は、ユーザーズガイドの「外部メディア自動暗号」の章を参照してください。